



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/706,629	11/12/2003	Joseph D. Wong	10013526-1	7991

22879 7590 10/17/2007
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER

REZA, MOHAMMAD W

ART UNIT	PAPER NUMBER
----------	--------------

2136

MAIL DATE	DELIVERY MODE
-----------	---------------

10/17/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/706,629

Applicant(s)

WONG, JOSEPH D.

Examiner

Mohammad W. Reza

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 July 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1 and 4-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1, and 4-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This is in response to the arguments filed on 07/30/2007.
2. Claims 1, and 4-24 are pending in the application.
3. Claims 1, and 4-24 have been rejected.

Response to Amendment

4. The examiner approves the amendments made to claim 1, 17, and 22.

Response to Arguments

5. Applicant's arguments filed on 07/30/2007 have been fully considered but they are not persuasive.

Applicant argues that the Williams does not disclose "...the second result derived from two or more enterprises in the relevant peer group". Examiner respectfully disagrees. Williams actually teaches this limitation in his inventions. For example, "FIG. 1 is a schematic block diagram of a global network according to one embodiment of the invention. The global network may include a plurality of internal networks 16 coupled to each other over a public internet 18 or a private wide area network 20. The global network also includes a prevention-based network security audit system that provides an automated assessment of security and regulatory policies, network vulnerability analysis, and makes recommendations for improving the security of the global

Art Unit: 2136

network. According to one embodiment of the invention, the prevention-based network security audit system ("the system") includes **a central compliance server 10 coupled to a database server 11 hosting an audit repository 14. The compliance server 10 is further coupled to one or more audit servers 12 over data communication lines 13.** According to one embodiment of the invention, the data communication lines transmit data in accordance with a transport layer security (TLS) protocol making use of encryption mechanisms, such as, for example, public key cryptography, to help ensure privacy between communicating applications.....The audit servers 12 are preferably strategically deployed around the global network to gather facts about wired 16 or wireless 22 local networks within the global network. According to one embodiment of the invention, the audit servers 12 are configured to gather facts relating to the wired and/or wireless 22 local networks using heterogeneous information sources. Such information sources may include scanners, cameras, manually entered data, and/or the like. The data gathered by each information source is converted into a normalized data format, such as, for example, and XML (Extensible Markup Language), and stored in the audit repository 14 for access by the compliance server 10. According to one embodiment of the invention, **the audit servers 12** are configured to provide DTAS

Art Unit: 2136

(Dynamic Target Acquisition Service) and/or DPF (Dynamic Packet Filter) services for the global network. DTAS allows unique network devices to be enumerated and their characteristics correlated over time even in DHCP (Dynamic Host Configuration Protocol) environments where their IP addresses may change. **DPF provides a firewall between the enterprise LAN/WAN and the private subnet containing the compliance server 10 and audit repository 14. DTAS and DPF may be provided via one or more dedicated servers, or as part of one or more audit servers 12. The compliance server 10 is coupled to the audit servers 12 and the audit repository 14 for tracking, from a central location, the overall health of the global network in terms of security and/or regulation compliance.** The compliance server 10 analyzes data gathered by the audit servers 12, and assesses policy violations and vulnerability risks, and makes recommendations for improving the security and policies of the network. The compliance server 10 further aids in the creation, configuration, editing, testing, and deployment of security and regulation policies for use during the network audits. The compliance server 10 also provides consolidated visibility into the security of the network and the various assessments that have been made about policy compliance, via various types of reports that may be generated manually or automatically based on

Art Unit: 2136

predetermined conditions (paragraphs 0060-0063)". From all these cited paragraphs it is clear that each one of these audit servers acting as an individual enterprise which are separated by firewall in between them. This limitation is more clearly described in the following paragraphs. ".....According to the illustrated embodiment, the compliance server includes a management interface 30, policy lab 32.....FIG. 3 is a more detailed functional block diagram of the policy lab 32 according to one embodiment of the invention. According to the illustrated embodiment, the policy lab includes a policy-editing module 40, policy library 42, and a policy deployment module 44. The policy library 42 is a repository of pre-established policies that are written in both English and in a machine-processable language. A policy is made up of one or more rules stored in the policy library 42. According to one embodiment of the invention, the policy library physically resides in the repository 14. The policies stored in the policy library 42 are designed to help meet the exacting standards of industry organizations such as the government, healthcare organizations, financial service organizations, technology sectors, international organizations, and/or public interest organizations. Exemplary policies defined by the government include NIST (National Institute of Standards and Technology), NSA (National Security Agency), OMB (Office of

Art Unit: 2136

Management and Budget), GLBA (Graham, Leach, Bliley Act), GISRA (Government Information Security Reform Act), Sarbanes-Oxley, FERC (Federal Energy Regulatory Commission), DITSCAP (DoD Information Technology Security Certification and Accreditation), and HIPAA (Health Insurance Portability and Accountability Act) (paragraphs, 0066-0073)". So it is clear that policy lab which consists of policy repository resides in the compliance server. All the standard enterprises information are pre-stored in the policy library. So Williams teaches this limitations.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1, and 4-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Williams et al hereafter Williams (patent application 20050257267) in view of Tonelli et al hereafter Tonelli (US Patent 6229540).

7. As per claim 1, Williams discloses a method comprising: collecting security information from the nodes of the enterprise under audit; analyzing the security information and providing a first result of this analysis; and a second result comprising

Art Unit: 2136

security standards applicable to the enterprise under audit and one or more other enterprises that together form a relevant peer group, the result indicating the relative security of the enterprise under audit relative to that of the peer group of enterprises (paragraphs, 0010, 0007). Although, Williams discloses comparing the results (paragraphs, 0101), he does not explicitly disclose comparing this first result with a second result. Nevertheless, it is well known in the network security art at the time of invention that auditing result to be compared with a standard result. Exemplary of this is Tonelli who discloses comparing this first result with a second result (col. 4, lines 27-42, col. 22, lines 8-19).

Accordingly, it would be obvious to one of ordinary skill in the network security art at the time of invention was made to have incorporated Tonelli's teachings of auditing networks with the teachings of Williams, for the purpose of suitably using the auditing result to compare with a standard result (col. 4-6).

10. As per claim 4, Williams discloses the method comprising the step of generating at least one report that presents the first and second results (paragraphs, 0010, 0007). He does not disclose arranged in a way that facilitates their comparison. However, Tonelli discloses arranged in a way that facilitates their comparison (col. 4, lines 27-42, col. 22, lines 8-19).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 4.

11. As per claim 5, Williams discloses the method wherein the generating step includes presenting the first and second results each broken down into several results

relating to several different areas of security, with a first and a second result presented for each different area of security (paragraphs, 0010, 0007). He does not disclose arranged in a way that facilitates their comparison. However, Tonelli discloses arranged in a way that facilitates their comparison (col. 4, lines 27-42, col. 22, lines 8-19).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 5.

12. As per claim 6, Williams discloses the method wherein, in the generating step, the results relating to several different areas of security comprise results arising from analysis of personnel security information and physical security information, at least some of the information included in the first result having been gathered using interviews during the collecting step (paragraphs, 106, 107).

13. As per claim 7, Williams discloses the method wherein, in the generating step, the results relating to several different areas of security comprise results arising from analysis of password security information and file access permission security information (paragraphs, 0121).

14. As per claim 8, Williams discloses the method wherein, in the generating step, the results relating to several different areas of security further comprise results arising from analysis of personnel security information and physical security information, at least some of the information included in the first result having been gathered using interviews during the collecting step (paragraphs, 106, 107).

15. As per claim 9, Williams discloses the method wherein, in the generating step, the several different areas of security comprise one or more results of analysis of node

configuration security information and one or more results of analysis of security information gathered using interviews (paragraphs, 106, 107).

16. As per claim 10, Williams discloses the method wherein, in the generating step, the one or more results of analysis of node configuration security information comprise results arising from analysis of password security information (paragraphs, 0010, 0007).

17. As per claim 11, Williams discloses the method wherein, in the generating step, the one or more results of analysis of node configuration security information comprises results arising from analysis of file access permission security information (paragraphs, 0010, 0007).

18. As per claim 12, Williams discloses the method wherein, the generating step generates at least two reports in different formats for different requesting parties or uses, and in particular one for technical experts that includes technical language and details and another for non-technical-experts that substantially excludes technical language and details (paragraphs, 0010, 0007). He does not disclose in the comparative of two results. However, Tonelli discloses comparative of two results (col. 4, lines 27-42, col. 22, lines 8-19).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 12.

19. As per claim 13, Williams discloses the method to which is added: generating and executing commands to alter the security information of one or more nodes to improve system security in at least some cases when the analysis or comparison or both indicate security is in need of improvement (paragraphs, 0010, 0007).

20. As per claim 14, Williams discloses the method comprising; generating at least one report that presents the first and second results (paragraphs, 0010, 0007). He does not disclose arranged in a way that facilitates their comparison. However, Tonelli discloses arranged in a way that facilitates their comparison (col. 4, lines 27-42, col. 22, lines 8-19).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 14.

21. As per claim 15, Williams discloses the method wherein the generating commands step generates commands which force the deactivation or correction of one or more passwords when the analysis or comparison or both indicate that these one or more passwords are not sufficiently secure (paragraphs, 0010, 0007).

22. As per claim 16, Williams discloses the method wherein the generating commands step generates commands which force alteration of one or more configuration file or control file access permissions if the analysis or comparison or both indicate that the access permissions assigned to these one or more files do not provide adequate system security (paragraphs, 0010, 0007).

23. As per claim 17, Williams discloses a system for auditing the security of an enterprise comprising: a plurality of nodes within the enterprise under audit; collectors associated with the nodes and arranged to collect from the nodes information concerning the security of the enterprise under audit;
a security analyzer arranged to analyze the information concerning the security of the enterprise under audit and to provide a first result of this analysis; a data base

Art Unit: 2136

containing a second result comprising security standards applicable to the enterprise under audit and one or more other enterprises that together form a relevant peer group; to determine the relative security of the enterprise under audit in comparison to that of the enterprises in the relevant peer group (paragraphs, 0010, 0007). Although, Williams discloses comparing the results (paragraphs, 0101), he does not explicitly disclose comparing this first result with a second result. Nevertheless, it is well known in the network security art at the time of invention that auditing result to be compared with a standard result. Exemplary of this is Tonelli who discloses a comparison mechanism arranged to compare the first and second results (col. 4, lines 27-42, col. 22, lines 8-19). The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 17.

24. As per claim 18, Williams discloses a system to which is added: a report generator that generates at least one report which presents the first and second results arranged each broken down into several results relating to several different areas of security, with a first and second result presented for each different area of security and arranged in a way (paragraphs, 0010, 0007). He does not disclose arranged in a way that facilitates their comparison. However, Tonelli discloses arranged in a way that facilitates their comparison (col. 4, lines 27-42, col. 22, lines 8-19).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 18.

25. As per claim 19, Williams discloses a system to which is added: change agents associated with the nodes and able to execute commands that alter node configuration

information; and a command generator that provides commands to the change agents on selected nodes to alter node configuration information to improve system security in response to the analyzer or comparison mechanism or both determining security improvements are needed (paragraphs, 106, 107).

26. As per claim 20, Williams discloses a system wherein the command generator includes a mechanism that can generate commands which, when executed, cause one or more of the change agents to force the deactivation or correction of one or more secure passwords if the security analyzer or comparison mechanism or both determine that one or more passwords are not sufficiently secure (paragraphs, 106, 107).

27. As per claim 21, Williams discloses a system wherein the command generator includes ~ a mechanism that can generate commands which, when executed, cause one or more of the change agents to force the alteration of the access permissions of one or more configuration files or control files if the security analyzer or comparison mechanism or both determine that the access permissions assigned to one or more such files do not provide sufficient security (paragraphs, 0010, 0007).

28. As per claim 22, Williams discloses a system for auditing the security of an enterprise comprising: a plurality of nodes within an enterprise under audit; collector means associated with the nodes for collecting information from the nodes concerning the security of the enterprise under audit;
security analyzer means for analyzing the information concerning the security of the enterprise under audit and for providing a first result of this analysis; data base means for storing and for presenting a second result comprising security standards applicable

Art Unit: 2136

to the enterprise under audit and one or more other enterprises that together form a relevant peer group; determine the relative security of the enterprise under audit in comparison to that of the enterprises in the relevant peer group (paragraphs, 0010, 0007). Although, Williams discloses comparing the results (paragraphs, 0101), he does not explicitly disclose comparing this first result with a second result. Nevertheless, it is well known in the network security art at the time of invention that auditing result to be compared with a standard result. Exemplary of this is Tonelli who discloses comparison means for comparing the first and second results (col. 4, lines 27-42, col. 22, lines 8-19).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 22.

29. As per claim 23, Williams discloses a system to which is added report generation means for generating at least one report which presents the first and second results each broken down into several results relating to several different areas of security, with a first and second result presented for each different area of security (paragraphs, 0010, 0007). He does not disclose arranged in a way that facilitates their comparison.

However, Tonelli discloses arranged in a way that facilitates their comparison (col. 4, lines 27-42, col. 22, lines 8-19).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 23.

30. As per claim 24, Williams discloses a system to which is added change agent means associated with the nodes for executing commands that alter node configuration

Art Unit: 2136

information; and

command generator means for providing commands to the change agent means on selected nodes as needed to alter system configuration information to improve system security in response to the security analyzer means or the comparison means or both determining that security improvements are needed (paragraphs, 0010, 0007).

Conclusion

31. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad w. Reza whose telephone number is 571-272-6590. The examiner can normally be reached on M-F (9:00-5:00).

Art Unit: 2136


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, MOAZZAMI NASSER G can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mohammad Wasim Reza

AU 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


10,15,07